IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

CHRISTINE COX, Individually and on behalf of all others similarly situated,	**Civil Action No. 1:25-cv-442**
Plaintiff,	**CLASS ACTION COMPLAINT**
vs.	
MARLBORO-CHESTERFIELD PATHOLOGY, P.C.	**JURY TRIAL DEMANDED**
Defendant.	

CLASS ACTION COMPLAINT

Plaintiff, Christine Cox, by and through undersigned counsel, brings this action against Marlboro-Chesterfield Pathology, P.C. ("MCP" or "Defendant") on behalf of herself and all others similarly situated, and makes the following allegations based upon information, attorney investigation and belief, and upon Plaintiff's own knowledge.

PRELIMINARY STATEMENT

1. Plaintiff brings this class action lawsuit against Defendant due to its failure to properly secure and safeguard sensitive and confidential personally identifiable information ("PII"), including names, dates of birth, Social Security numbers and protected health information of its current and former employees. Defendant's wrongful disclosure has harmed Plaintiff and the Classes (defined below), which include nearly 235,000 people.

2. Medical and financial records represent the most sensitive information available concerning a person's private affairs. These records reveal intimate and personal aspects of the human condition, such as illnesses that might carry social stigma and details about substance abuse, family planning and mental health. Congress has passed legislation under the Health Insurance

Portability and Accountability Act of 1996 ("HIPAA") in order to protect this highly confidential data, because in the wrong hands, bad actors may target and exploit the most sensitive and vulnerable populations among the public.

3. Defendant is an anatomic pathology laboratory located in Pinehurst, NC. MCP has Anatomic/Clinical Board-certified pathologists with experience or specialty training in gastrointestinal, cytopathology, dermatology, urology and surgical pathology.

4. Defendant had an obligation to safeguard the information used when providing its services. On or around January 16, 2025, Defendant experienced unauthorized activity on their internal IT systems. Based on their subsequent investigation, they determined that an unauthorized party accessed their systems and acquired certain records ("Data Breach").[1] MCP waited over four months before informing the public on or about May 22, 2025.[2]

5. Defendant knew or should have known of the increasing number of well-publicized data breaches that have occurred in the United States. And yet, Defendant failed to adequately secure and upgrade its systems, allowing another breach to occur, this time compromising consumer Personal Information.

6. Plaintiff and members of the Classes ("Class Members") entrusted Defendant with their sensitive and valuable Personal Information. Plaintiff and Class Members did not know that Defendant's data security was inadequate. They did not expect that by obtaining services from MCP, they would suffer serious injury that would last for years after their coverage.

7. Defendant has caused harm to Plaintiff and Class Members by collecting, using, and maintaining their Personal Information for its own economic benefit but utterly failing to protect that information: Defendant did not maintain adequate security systems, did not properly archive Personal Information, allowed access by third parties, and did not implement sufficient security measures.

[1] *See* Notice of Security Incident; https://mcpathology.com/wp-content/uploads/MC_Pathology_BreachNotice_2025.pdf **Exhibit A**
[2] *Id.*

8. Plaintiff brings this action on behalf of all persons in the United States whose Personal Information was compromised as a result of Defendant's failure to:

i) adequately protect its employees' Personal Information;

ii) warn employees of its inadequate information security practices; and

iii) effectively secure hardware, data, and information systems through reasonable and effective security procedures.

9. Defendant's conduct constitutes negligence that proximately caused damages to Plaintiff and Class Members.

10. Plaintiff and Class Members have suffered injury as a direct and proximate result of Defendant's conduct.

11. These above-mentioned injuries to Plaintiff and the Class Members include:

a) lost or diminished value of Personal Information, a form of property that Defendant obtained from Plaintiff and Class Members;

b) out-of- pocket expenses associated with preventing, detecting, and remediating identity theft and other unauthorized use of their Personal Information;

c) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time;

d) the continued and certain increased risk that unauthorized persons will access and abuse Plaintiff and Class Members' unencrypted Personal Information that is available on the dark web; (v) the continued and certain increased risk that the Personal Information that remains in Defendant's possession is subject to further unauthorized disclosure for so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information;

e) invasion of privacy; and

f) theft of their Personal Information and the resulting loss of privacy rights in that information.

12. As a direct and proximate result of Defendant's breach of confidence and failure to protect the Personal Information, Plaintiff and Class Members have been injured by facing

ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuses of their Personal Information; ongoing monetary loss and economic harm; loss of value of privacy and confidentiality of the stolen Personal Information; illegal sales of the compromised Personal Information; mitigation expenses and time spent on credit monitoring; identity theft insurance costs; credit freezes/unfreezes; expense and time spent on initiating fraud alerts and contacting third parties; decreased credit scores; lost work time; and other injuries. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

Plaintiff

13. Plaintiff Christine Cox is a citizen of Rockingham, North Carolina. Rockingham is located in Richmond County.

14. Defendant retained and stored Plaintiff's Personal Information and PHI on its computer systems, including the systems affected by the Data Breach.

15. Had Plaintiff known that Defendant does not adequately protect the PII/PHI in its possession, they would not have obtained services from Defendant or agreed to provide them with their Personal Information.

16. Plaintiff received a written form of a notice from MCP about being affected by the Data Breach.

17. Plaintiff is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

18. Plaintiff suffered actual injury from having their Personal Information compromised as a result of the Data Breach including but not limited to (a) damage to and diminution in the value of Plaintiff' Personal Information, a form of property that Defendant obtained from Plaintiff; (b) violation of Plaintiff' privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

19. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. As a result of the Data Breach, Plaintiff will continue to be at increased risk of identity theft and fraud for years to come.

Defendant

20. Defendant Marlboro-Chesterfield Pathology, P.C., is a South Carolina corporation with its principal offices located at 30 Page St, Pinehurst, North Carolina, 28374.

JURISDICTION AND VENUE

21. This Court possesses subject-matter jurisdiction to adjudicate the claims set forth herein under the provisions of the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are members of the Class who are diverse from Defendant, and (4) there are more than 100 Class Members.

22. This Court has personal jurisdiction over this action because Defendant has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District such that it could reasonably foresee litigation being brought in this District.

23. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391 because Defendants transact their business in this District, and a substantial part of the events and/or omissions giving rise to the claims occurred, in part, within this District.

FACTUAL ALLEGATIONS

Injury to Plaintiff and Class Members

24. Plaintiff is an individual who had their Personal Information compromised in the Data Breach and brings this action on behalf of themselves and all those similarly situated both across the U.S. and within their state or territory of residence.

25. Plaintiff recently had over $200 in fraudulent charges attempted on her credit card.

26. Because Defendant has exclusive knowledge of what information was compromised for each individual Class Member, Plaintiff reserves the right to supplement her allegations with additional facts and injuries as they are discovered.

27. Plaintiff has suffered actual injury and one or more concrete (real and not abstract), imminent and particularized injuries described below as a direct and proximate result of Defendant's known deficient data security and failure to protect Plaintiff's Personal Information, as well as Defendant's concealment of the same, that allowed unauthorized access to Plaintiff' Personal Information.

28. Had Defendant disclosed that it disregarded its duty to protect Plaintiff' Personal Information or otherwise had insufficient security measures to safeguard and protect Plaintiff' Personal Information from unauthorized access, Plaintiff would have taken this into account in making their decisions.

29. Had Plaintiff and the Classes known that providing Personal Information to Defendant would result in their Personal Information being compromised and exfiltrated, Plaintiff and the Classes would not have purchased the products or services, or would have paid less for them, or would not have provided some or all of their Personal Information to Defendant. Thus, Plaintiff and the Classes significantly overpaid based on what the products were represented to be compared to what Plaintiff and the Classes actually received.

30. In addition to actual, present, concrete, and current injuries described below, because of Defendant's actions and omissions, each and every Plaintiff has suffered, and will continue to suffer perpetual emotional distress, worry, other emotional or psychological harm, and well- founded fear that additional, realistic, objectively-reasonable, threatened, impending, sufficiently imminent harm in the form of identity theft or fraud will occur in the future.

31. Plaintiff has invested, and will continue in perpetuity to invest, time and money into precautionary measures that could, but may not successfully, mitigate the potential misuse of their data.

32. The Data Breach was the product of an intentional criminal act to gain access to the data. It was the result of a sophisticated, intentional, and malicious attack by professional cybercriminal hackers and was not the result of an accidental disclosure. Thus, there is an increased and substantial risk that the victims will experience identity theft or fraud that is sufficiently imminent.

33. On information and belief, an unauthorized actor accessed Defendant's network on or around January 16, 2025.[3]

34. Upon information and belief, the Personal Information stolen in the Data Breach included information such as birth dates, medical treatment information, and health insurance information, such as policy numbers, and full names that thieves are likely to use to perpetrate identity theft or fraud now or at any time in the future.

35. The concreteness of the injury included traditional harms such as monetary harm recognized as a basis for a lawsuit in American courts.

36. Plaintiff was also injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuse of this Personal Information, resulting in ongoing monetary loss and economic harm, loss of value of privacy and confidentiality of the stolen Personal Information, illegal sales of the compromised Personal Information, mitigation expenses and time spent on credit monitoring, identity theft insurance, credit freezes/unfreezes, expenses and time spent in initiating fraud alerts, contacting third parties; decreased credit scores, and lost work time.

37. The dark web is a portion of the internet that facilitates criminal activity worldwide and functions as an underground illicit market for the sale of sensitive stolen data and illegal products such as drugs, weapons, and counterfeit money.[4]

[3] https://mcpathology.com/wp-content/uploads/MC_Pathology_BreachNotice_2025.pdf
[4] https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html (last accessed May 29, 2025)

38. There are strong indications that the Personal Information exfiltrated from Defendant's network has been published and is still being offered for download and/or sale on underground marketplaces.

39. As a result of the Data Breach, Plaintiff and the Classes have received a high-volume of phishing emails and spam telephone calls. Such scams trick consumers into giving account information, passwords, and other valuable personal information to scammers. This significantly increases the risk of further substantial damages to Plaintiff and the Classes, including, but not limited to, monetary and identity theft.

40. Plaintiff has spent time and effort researching the breach after having received notice of her vulnerability of said breach. Plaintiff and Class Members' awareness of their substantial risk for identity theft has caused emotional distress.

Overview of Defendant and its Data Breach

41. On or about May 22, 2025, Defendant sent Plaintiff and Class Members a notice of the Data Breach (the "Notice of Security Incident"), informing them that:

> ***"What Happened?***
>
> On or around January 16, 2025, we experienced unauthorized activity on certain of our internal IT systems. Based on our subsequent investigation, we determined that an unauthorized party accessed our systems and acquired certain records from our systems. We took prompt action and quickly engaged third-party specialists to assist us in securing our systems and investigating the incident. Law enforcement is aware of the incident and we have cooperated with their investigation. The involvement of law enforcement did not delay this notification. Through a thorough investigation and extensive review of the impacted data, which concluded on March 31, 2025, we determined that some of your personal information was contained in the affected records. We took steps, to the best of our ability and knowledge, to ensure that the data taken by the unauthorized party was deleted.
>
> ***What Information Was Involved?***
>
> The impacted information varies by individual, and may have included: name, address, date of birth, medical treatment information, and health insurance

information, such as policy numbers. As of this writing, we have not received any reports of identity theft related to this incident.

What We Are Doing.

Marlboro-Chesterfield Pathology, P.C. has conducted a thorough review of the potentially affected records and systems. Upon becoming aware of the incident, we promptly began taking steps to secure and restore all affected systems, and began an investigation to understand the scope and impact of the incident. We worked with thirdparty forensic specialists to investigate the incident. We have implemented measures to contain the unauthorized access and further strengthen the security of our networks."

Marlboro-Chesterfield Pathology, P.C. Violated HIPAA's Requirements to Safeguard Data

42. Defendant had duties to ensure that all information it collected and stored was secure, and that it maintained adequate and commercially reasonable data security practices to ensure the protection of plan members' Personal Information.

43. Defendant is covered by HIPAA (see 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

44. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. See 45 C.F.R. § 160.103.

45. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

46. HIPAA requires that Defendant implements appropriate safeguards for this information.

47. HIPAA requires that Defendant provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—i.e., non-encrypted data. Such notice is to be provided without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

48. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. See 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* U.S. Department of Health & Human Services, Security Rule Guidance Material.[5] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-PHI." *See* U.S. Department of Health & Human Services, Guidance on Risk Analysis.[6]

49. Should a health care provider experience an unauthorized disclosure, it is required to conduct a four-factor Risk Assessment (HIPAA Omnibus Rule: "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported."). The four-factor risk assessment focuses on:

a) the nature and extent of the PHI involved in the incident (*e.g.,* whether the incident involved sensitive information like social security numbers or infectious disease test results);

[5] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html. (last accessed May 29, 2025)
[6] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last accessed May 29, 2025)

b) the recipient of the PHI;

c) whether the PHI was actually acquired or viewed; and,

d) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (*e.g.*, whether it was immediately sequestered and destroyed)."[7]

50. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

51. Despite these requirements, Defendant failed to comply with its duties under HIPAA and its own Privacy Practices. Indeed, Defendant failed to:

a) Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b) Adequately protect Plaintiff and the Class Members' Personal Information;

c) Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d) Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e) Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f) Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

[7] 78 Fed. Reg. 5641-46; *see also* 45 C.F.R. § 164.304.

g) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h) Take safeguards to ensure that Defendant's business associates adequately protect protected health information;

i) Conduct the four-factor Risk Analysis following the Data Breach;

j) Properly send timely notice to Plaintiff and the Classes pursuant to 45 C.F.R.§§ 164.400-414;

k) Ensure compliance with the electronically protected health information security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

l) Train all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out its functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

52. Defendant failed to comply with its duties under HIPAA and its own privacy policies despite being aware of the risks associated with unauthorized access of members' Personal Information.

Defendant Was on Notice That Highly Valuable Personal Information of Its Patients Could Be Breached

53. Defendant was, or should have been, aware that it was collecting highly valuable data, for which Defendant knew, or should have known, there is an upward trend in data breaches in recent years.[8] Accordingly, Defendant was on notice of the harms that could ensue if it failed to protect patients' data.

[8] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last accessed Jan 18, 2024) ("Our healthcare statistics clearly show there

54. As early as 2014, the FBI alerted the healthcare industry that they were an increasingly preferred target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (Personal Information)" so that these companies can take the necessary precautions to thwart such attacks.[9]

55. Personal Information is a valuable commodity to identity thieves. Compromised Personal Information is traded on the "cyber black-market." As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, social security numbers and other Personal Information directly on various dark web sites making the information publicly available.[10]

56. Further, medical databases are particularly high value targets for identity thieves. According to one report, a stolen medical identity has a $50 street value on the black market, whereas a social security number sells for only $1.[11]

Consequences of the Data Breach for Consumers/Employees

57. Plaintiff and Class Members have suffered actual harm and will continue to be harmed as a result of Defendant's conduct. Defendant failed to institute adequate security measures and neglected system vulnerabilities that led to the Data Breach. Defendant's failure to keep Plaintiff and Class Members' Personal Information secure has severe ramifications. Given the sensitive nature of the Personal Information stolen in the Data Breach – names, addresses,

---

has been an upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published.").

[9] Reuters, *FBI warns healthcare firms they are targeted by hackers*, August 20, 2014, http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820

[10] Here's How Much Your Personal Information Is Selling for on the Dark Web, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed May 30, 2025); McFarland et al., The Hidden Data Economy, at 3, available at https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf (last accessed May 30, 2025)

[11] Study: Few Aware of Medical Identity Theft Risk, Claims Journal (June 14, 2012), https://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last accessed May 30, 2025)

dates of birth, social security numbers, driver's license numbers and/or other government-issued ID numbers, health insurance information, Medicaid/Medicare ID numbers, and medical records – hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future. Plaintiff and Class Members may be subject to blackmail from nefarious actors concerning the disclosure of their medical records. As a result, Plaintiff and Class Members have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

58. Plaintiff's stolen Personal Information may now be circulating on the dark web and it is highly valuable. Malicious actors use Personal Information to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use consumers' Personal Information to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create synthetic identities.

59. Theft of social security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their social security number, and a new social security number will not be provided until after the harm has already been suffered by the victim.

60. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other Personal Information (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME Magazine quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have

your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[12]

61. Further, malicious actors often wait months or years to use the Personal Information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen Personal Information, meaning individuals can be the victim of several cybercrimes stemming from a single data breach. Moreover, although elements of some of Plaintiff and Class Members' data may have been compromised in other data breaches, the fact that the Data Breach centralizes the Personal Information and identifies the victims as Defendant's current, former, or prospective customers materially increases the risk to Plaintiff and the Classes.

62. Theft of Personal Information is even more serious when it includes theft of PHI. A report published by the World Privacy Forum and presented at the U.S. FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

i) Theft of Personal Information is even more serious when it includes theft of PHI. A report published by the World Privacy Forum and presented at the U.S. FTC Workshop on Informational Injury describes what medical identity theft victims may experience: Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

ii) Significant bills for medical goods and services neither sought nor received.

iii) Issues with insurance, co-pays, and insurance caps.

iv) Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

[12] Patrick Lucas Austin, 'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/ (last accessed May 29, 2025).

v) Serious life consequents resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

vi) As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

vii) Phantom medical debt collection based on medical billing or other identity information.

viii) Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[13]

63. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft,"[14] and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[15] Moreover, there is often a significant lag time between when a person suffers harm due to theft of their Personal Information and when they discover the harm. Plaintiff and Class Members will therefore need to spend time and money to continuously monitor their accounts for years to ensure the Personal Information obtained in the Data Breach is not used to harm them. Plaintiff and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high- quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendant's Data Breach. In other words, Plaintiff and Class Members have been harmed by the value of identity protection services they must purchase in the future to ameliorate the risk of harm they now face due to the Data Breach.

[13] Pam Dixon and John Emerson, The Geography of Medical Identity Theft, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf
[14] https://www.gao.gov/assets/a262904.html (last accessed May 29, 2025)
[15] *Id.*

64. Plaintiff and Class Members have also been harmed and damaged in the amount of the market value of the hacker's access to their Personal Information that was permitted without authorization by Defendant. This market value for access to Personal Information can be determined by reference to both legitimate and illegitimate markets for such information.

65. In sum, Plaintiff and Class Members were injured as follows:

a) theft of their Personal Information and the resulting loss of privacy rights in that information;

b) improper disclosure of their Personal Information;

c) loss or diminished value of their Personal Information;

d) the lost value of access to Plaintiff' and Class Members' Personal Information permitted by Defendant;

e) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendant's Data Breach;

f) Defendant's retention of profits attributable to Plaintiff and Class Members' Personal Information that Defendant failed to adequately protect;

g) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom;

h) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach;

i) overpayments to Defendant for goods and services purchased, as Plaintiff and Class Members reasonably believed a portion of the price they paid for those goods and services would fund reasonable security measures that would protect their Personal Information, which was not the case; and

j) nominal damages.

CLASS ACTION ALLEGATIONS

NATIONWIDE CLASS

66. Plaintiff brings this action on behalf of themselves individually and also as a class action on behalf of themselves and all similarly situated, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, including specifically on behalf of the following Classes:

> **All persons residing in the United States whose Personal Information was maintained on Defendant's systems that were compromised as a result of the breach announced by Defendant on or around May 22, 2025.**

67. This definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

STATEWIDE SUBCLASS

68. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiff brings this case as a class action and brings pertinent statutory or common law claims on behalf of the following North Carolina Subclass (the "Subclass") as defined as follows:

> **All persons residing in North Carolina whose Personal Information was maintained on Marlboro-Chesterfield Pathology, P.C.'s systems that were compromised as a result of the breach announced on or around May 22, 2025.**

69. This definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

70. Excluded from the Nationwide Class and the Subclass are Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

71. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

72. **Numerosity:** The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. Plaintiff is informed and believes there are thousands of members of the Class, the precise number being unknown to Plaintiff, but such number being ascertainable from Defendant's records. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

73. **Commonality and Predominance:** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include, but are not limited to, the following:

a) Whether Defendant represented to Plaintiff and Class Members that Defendant would protect Plaintiff and the Class Members' Personal Information;

b) Whether Defendant owed a duty to Plaintiff and Class Members to exercise due care in collecting, storing, and safeguarding their Personal Information;

c) Whether Defendant breached a duty to Plaintiff and Class Members to exercise due care in collecting, storing, and safeguarding their Personal Information;

d) Whether Defendant has a contractual obligation to safeguard Plaintiff and Class Members' Personal Information;

e) Whether Defendant's conduct breached any contractual obligation to protect Plaintiff and Class Members' Personal Information;

f) Whether Defendant knew or should have known that its systems were vulnerable to a data breach;

g) Whether Defendant was negligent in failing to implement reasonable and adequate security procedures and practices;

h) Whether Defendant's security measures to protect its systems were reasonable in

light of known legal requirements;

i) Whether Defendant notified Plaintiff and Class Members that their Personal Information had been compromised as soon as practicable and without unreasonable delay after the Data Breach was discovered;

j) Whether the content of Defendant's notice to Plaintiff and Class Members that their Personal Information had been compromised was adequate in light of known legal requirements;

k) Whether Defendant violated its common law duties to Plaintiff and Class Members by failing to promptly notify Plaintiff and Class Members that their Personal Information had been compromised;

l) Whether Defendant adequately addressed the vulnerabilities that permitted the Data Breach to occur;

m) Whether Defendant's conduct injured Plaintiff and the Class Members;

n) Whether Defendant's conduct violated HIPAA laws;

o) Whether Defendant's conduct violated state consumer protection laws;

p) Whether Defendant's conduct violated the laws of North Carolina;

q) Whether Defendant's conduct violated state data privacy laws;

r) Whether Defendant's conduct violated state data breach laws;

s) Whether Plaintiff and Class Members are entitled to actual damages and/or punitive damages as a result of Defendant's wrongful conduct;

t) Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

u) Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

74. **Typicality:** As to each Class and Subclass, Plaintiff's claims are typical of other Class Members' claims because Plaintiff and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way. Plaintiff's Personal Information was

in Defendant's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to those of other Class Members and Plaintiff seeks relief consistent with the relief of the Classes.

75. **Adequacy:** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Classes because Plaintiff is a member of the Classes and is committed to pursuing this matter against Defendant to obtain relief for the Classes. Plaintiff has no conflicts of interest with the Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class Members interests.

76. **Superiority:** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual Plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class Members are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

77. The Class also may be certified because Defendants have acted or refused to act on grounds applicable to the Class, thereby making appropriate final declaratory and/or injunctive relief with respect to the members of the Class as a whole.

78. Plaintiff seeks preliminary and permanent injunctive and equitable relief on behalf of the entire Class, on grounds generally applicable to the entire Class, to enjoin and prevent Defendants from engaging in the acts described above, such as continuing to market and sell Products that may be defective. Further, Plaintiff seek for Defendants to provide a full refund of the purchase price of the Products to Plaintiff and the Class Members.

79. Unless a Class is certified, Defendants will retain monies received as a result of their conduct that was taken from Plaintiff and the Class Members. Unless a Class-wide injunction is issued, Defendants may continue to commit the violations alleged and the members of the Class and the general public will continue to be misled and placed in harms' way.

FOR A FIRST COLLECTIVE CAUSE OF ACTION

NEGLIGENCE
(Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Subclass)

80. Plaintiff realleges and incorporates by reference each and every allegation contained above, as if fully set forth herein.

81. Defendant collected sensitive Personal Information from Plaintiff and Class Members in connection with providing medical services.

82. Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendant's security systems to ensure that Plaintiff and Class Members' Personal Information in Defendant's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely

manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

83. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described herein.

84. Defendant had common law duties to prevent foreseeable harm to Plaintiff and the Class Members. These duties existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiff and Class Members would be harmed by Defendant's failure to protect their Personal Information because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendant knew that it was more likely than not Plaintiff and other Class Members would be harmed if it allowed such a breach.

85. Defendant's duty to use reasonable security measures also arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and Class Members, on the other hand. The special relationship arose because Plaintiff and Class Members entrusted Defendant with their Personal Information and sensitive healthcare information. Defendant alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

86. Defendant is covered by HIPAA (see 45 C.F.R. § 160.102) and, as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

87. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the

information can be used to identify the individual," that is held or transmitted by a healthcare provider. See 45 C.F.R. § 160.103.

88. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

89. HIPAA requires that Defendant implements appropriate safeguards for this information.

90. Defendant's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Personal Information by companies such as Defendant. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

91. Defendant admits that it has a responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the Personal Information at issue here.

92. Defendant knew or should have known that its computing systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential Personal Information.

93. Defendant also had a duty to safeguard the Personal Information of Plaintiff and Class Members and to promptly notify them of a breach because of state laws and statutes that require Defendant to reasonably safeguard sensitive Personal Information, as detailed herein.

94. Timely, adequate notification was required, appropriate and necessary so that, among other things, Plaintiff and Class Members could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial

institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Defendant's misconduct.

95. Defendant breached the duties they owed to Plaintiff and Class Members described above and thus was negligent. Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Personal Information of Plaintiff and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breach; (d) comply with regulations protecting the Personal Information at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiff and the Class Members' Personal Information in Defendant's possession had been or was reasonably believed to have been, stolen or compromised.

96. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their Personal Information would not have been compromised.

97. Defendant's failure to take proper security measures to protect the sensitive Personal Information of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiff and Class Members' Personal Information.

98. Plaintiff and Class Members were foreseeable victims of Defendant's inadequate data security practices, and it was also foreseeable that Defendant's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiff and Class Members as described in this Complaint.

99. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information;

illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; lost value of access to their Personal Information permitted by Defendant; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendant's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages and other economic and non- economic harm.

FOR A SECOND COLLECTIVE CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Subclass)

100. Plaintiff realleges and incorporates by reference each and every allegation contained above, as if fully set forth herein.

101. Defendant is covered by HIPAA (see 45 C.F.R. § 160.102) and, as such, is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

102. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. See 45 C.F.R. § 160.103.

103. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

104. HIPAA requires that Defendant implements appropriate safeguards for this information.

105. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, also prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant of failing to use reasonable measures to protect Personal Information.

106. The FTC publications and orders also form the basis of Defendant's duty.

107. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving a company as large as Defendant, including, specifically the damages that would result to Plaintiff and Class Members.

108. In addition, under state data security statutes, Defendant had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and Class Members' Personal Information.

109. Defendant's violation of HIPAA and Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

110. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

111. The harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Classes.

112. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff' and Class Members' Personal Information.

113. Plaintiff and Class Members were foreseeable victims of Defendant's violations of the HIPAA, the FTC Act, and state data security statutes. Defendant knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiff and Class Members' Personal Information would cause damage to Plaintiff and Class Members.

114. But for Defendant's violation of the applicable laws and regulations, Plaintiff and Class Members' Personal Information would not have been accessed by unauthorized parties.

115. As a direct and proximate result of Defendant's negligence per se, Plaintiff and Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; lost value of access to their Personal Information permitted by Defendant; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendant's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non- economic harm.

FOR A THIRD COLLECTIVE CAUSE OF ACTION
BREACH OF CONTRACT
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Subclass)

116. Plaintiff realleges and incorporates by reference each and every allegation contained above, as if fully set forth herein.

117. Defendant had valid contracts with various hospitals, clinics and healthcare providers. It also had contracts with its vendor. A principal purpose of all of those contracts was to securely store, transmit and safeguard the PII/PHI of Plaintiff and Class Members.

118. Upon information and belief, Defendant and each of the contracting hospitals and clinics expressed an intention that Plaintiff and Class Members were intended third party beneficiaries of these agreements.

119. Plaintiff and Class Members are also intended third party beneficiaries of these agreements because recognizing them as such is appropriate to effectuate the intentions of the parties, and the circumstances indicate that Defendant intended to give the beneficiaries the benefit of the promised performance.

120. Defendant breached its agreements with the contracting hospitals and clinics by allowing the data breach to occur, and as otherwise set forth herein.

121. Defendant's breach caused foreseeable and material damages to Plaintiff and Class Members.

FOR A FOURTH COLLECTIVE CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Subclass)

122. Plaintiff realleges and incorporates by reference each and every allegation contained above, as if fully set forth herein.

123. This Count is pleaded in the alternative to the Third Collective Cause of Action referenced above.

124. Defendant provides health care services to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct.

125. Through Defendant's provision of services, it knew or should have known that it must protect Plaintiff and Class Members' confidential Personal Information and PHI in accordance with Defendant's policies, practices, and applicable law, including the FTC Act and HIPAA.

126. As part of receiving services, Plaintiff and Class Members turned over valuable Personal Information and PHI to Defendant. Accordingly, Plaintiff and Class Members bargained with Defendant to securely maintain and store their Personal Information.

127. Defendant violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff and Class Members' Personal Information.

128. Plaintiff and Class Members have been damaged by Defendant's conduct, including by incurring the harms and injuries arising from the Data Breach now and in the future.

FOR A FIFTH COLLECTIVE CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Subclass)

129. Plaintiff realleges and incorporates by reference each and every allegation contained above, as if fully set forth herein.

130. Plaintiff and Class Members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by MCP and that was ultimately stolen in the Data Breach.

131. Defendant was benefited by the conferral upon it of the Personal Information pertaining to Plaintiff and Class Members and by its ability to retain, use, sell, and profit from that information. Defendant understood that it was in fact so benefited.

132. Defendant also understood and appreciated that the Personal Information pertaining to Plaintiff and Class Members was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that Personal Information.

133. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, that Personal Information would not have been transferred to and entrusted with Defendant.

134. Because of its use of Plaintiff and Class Members' Personal Information, Defendant sold more services and products than it otherwise would have sold. Defendant was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create to the detriment of Plaintiff and Class Members.

135. Defendant also benefited through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiff and Class Members' Personal Information.

136. Defendant also benefited through its unjust conduct in the form of the profits it gained through the use of Plaintiff and Class Members' Personal Information.

137. It is inequitable for Defendant to retain these benefits.

138. As a result of Defendant's wrongful conduct as alleged in this Complaint (including among things its failure to employ adequate data security measures, its continued maintenance and use of the Personal Information belonging to Plaintiff and Class Members without having adequate data security measures, and its other conduct facilitating the theft of that Personal Information), Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

139. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff and Class Members' sensitive Personal Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

140. It is inequitable, unfair, and unjust for Defendant to retain these wrongfully obtained benefits. Defendant's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

141. The benefit conferred upon, received, and enjoyed by Defendant was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for Defendant to retain the benefit.

142. Defendant's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiff and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their Personal Information and have caused Plaintiff and Class Members other damages as described herein.

143. Plaintiff and Class Members have no adequate remedy at law.

144. Defendant is therefore liable to Plaintiff and Class Members for restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically: the value to Defendant of the Personal Information that was stolen in the Data Breach; the profits Defendant received and is receiving from the use of that information; the amounts that Defendant overcharged Plaintiff and Class Members for the use of Defendant's products and services; and the amounts that Defendant should have spent to provide reasonable and adequate data security to protect Plaintiff and Class Members' Personal Information.

FOR A SIXTH COLLECTIVE CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Subclass)

145. Plaintiff realleges and incorporates by reference each and every allegation contained above, as if fully set forth herein.

146. As a condition of obtaining services from Defendant, Plaintiff and Class Members gave Defendant their Personal Information and PHI in confidence, believing that

Defendant would protect that information. Plaintiff and Class Members would not have provided Defendant with this information had they known their information would not be adequately protected. Defendant's acceptance and storage of Plaintiff and Class Members' Personal Information and PHI created a fiduciary relationship between Defendant and Plaintiff and Class Members. In light of this relationship, Defendant must act primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiff and Class Members' Personal Information and PHI. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship.

147. Defendant breached that duty by failing to properly protect the integrity of the systems containing Plaintiff and Class Members' Personal Information and PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff and Class Members' Personal Information and PHI that it collected, retained, and stored.

148. As a direct and proximate result of Defendant's negligence per se, Plaintiff and Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; lost value of access to their Personal Information permitted by Defendant; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendant's Data Breach; and lost benefit of their bargains and overcharges for services or products.

FOR A SEVENTH COLLECTIVE CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Subclass)

149. Plaintiff realleges and incorporates by reference each and every allegation contained above, as if fully set forth herein.

150. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

151. An actual controversy has arisen in the wake of the Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Personal Information. Plaintiff and Class Members continue to suffer injury as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future given the publicity around the Data Breach and the nature and quantity of the Personal Information stored by Defendant.

152. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

153. Defendant continues to owe a legal duty to secure consumers' Personal Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

154. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Personal Information.

155. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect consumers' Personal Information.

156. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach. The risk of another such breach is real, immediate, and substantial. If another data breach at MCP occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

157. The hardship to Plaintiff and Class Members, if an injunction does not issue, exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs at Defendant, Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

158. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and Class Members and the millions of consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of members of the Classes, pray for judgement in their favor and against Defendant as follows:

a) Certification of the action as a Class Action Pursuant to Federal Rule of Civil Procedure 23, and appointment of Plaintiff as Class Representative and her counsel of record as Class Counsel;

b) That acts alleged herein be adjudged and decreed to constitute negligence and violations of the consumer protection laws of Wisconsin.

c) A judgment against Defendant for the damages sustained by Plaintiff and the Classes defined herein, and for any additional damages, penalties, and other monetary relief provided by applicable law;

d) An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes, including, but not limited to:

e) Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

f) Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

g) Ordering that Defendant audits, tests, and trains its security personnel regarding any new or modified procedures;

h) Ordering that Defendant segments consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, unauthorized third parties cannot gain access to other portions of Defendant's systems;

i) Ordering that Defendant purge, delete, and destroy in a reasonably secure manner consumer data not necessary for their provisions of services;

j) Ordering that Defendant conducts regular database scanning; and

k) Ordering that Defendant routinely and continually conducts internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

l) By awarding Plaintiff and Class Members pre-judgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of the Complaint in this action;

m) The costs of this suit, including reasonable attorney fees; and

n) Such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of all those similarly situated, hereby requests a jury trial, pursuant to Federal Rule of Civil Procedure 38, on any and all claims so triable.

Dated: June 4, 2025

Respectfully Submitted,

/s/Ryan Valente
Ryan Valente (Bar ID No.: 40140)
Paul J. Doolittle*
POULIN | WILLEY | ANASTOPOULO, LLC
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
teamvalente@poulinwilley.com
cmad@poulinwilley.com
paul.doolittle@poulinwilley.com

Attorneys for Plaintiff Cox

*Pro Hac Vice Forthcoming